

PATENT COOPERATION TREATY

CORRECTED VERSION

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43bis.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/US2004/021530

International filing date (day/month/year)
01.07.2004

Priority date (day/month/year)
07.07.2003

International Patent Classification (IPC) or both national classification and IPC
H04L29/06, H04L12/56, H04N7/16

Applicant
QUALCOMM INCORPORATED

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☒ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:



European Patent Office - Gitschiner Str. 103
D-10958 Berlin
Tel. +49 30 25901 - 0
Fax: +49 30 25901 - 840

Authorized Officer

Figiel, B

Telephone No. +49 30 25901-473



**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**International application No.
PCT/US2004/021530**Box No. I Basis of the opinion**

1. With regard to the language, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
 - ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).
2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
 - a. type of material:
 - ☐ a sequence listing
 - ☐ table(s) related to the sequence listing
 - b. format of material:
 - ☐ in written format
 - ☐ in computer readable form
 - c. time of filing/furnishing:
 - ☐ contained in the international application as filed.
 - ☐ filed together with the international application in computer readable form.
 - ☐ furnished subsequently to this Authority for the purposes of search.
3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
4. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

 International application No.
PCT/US2004/021530

Box No. II Priority

 1. ☒ The following document has not been furnished:

☒ copy of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(a)).

☐ translation of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(b)).

Consequently it has not been possible to consider the validity of the priority claim. This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

 2. ☐ This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.

 3. ☐ It has not been possible to consider the validity of the priority claim because a copy of the priority document was not available to the ISA at the time that the search was conducted (Rule 17.1). This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

4. Additional observations, if necessary:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	3- 7,10- 11,14- 17,20-21,24-30,33-36,39-40,43-47,50-51,54-57,60-61
	No: Claims	1- 2,8-9, 12-13,18-19,22-23,31-32,37-38,41-42,48-49,52-53,58-59
Inventive step (IS)	Yes: Claims	
	No: Claims	1-61
Industrial applicability (IA)	Yes: Claims	1-61
	No: Claims	

2. Citations and explanations

see separate sheet

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING
AUTHORITY (SEPARATE SHEET)**

International application No.

PCT/US2004/021530

1. Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure:

D1: EP-A-1 001 570 (LUCENT TECHNOLOGIES INC) 17 May 2000 (2000-05-17)

D2: AL-TAWIL K ET AL: "A new authentication protocol for roaming users in GSM" PROCEEDINGS IEEE INTERNATIONAL SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS, XX, XX, 6 July 1999 (1999-07-06), pages 93-99, XP002168055

2. The present application does not meet the requirements of Articles 33(1)-(2) PCT, because the subject-matter of **independent claims 1, 12, 22, 31, 41 and 52** is **not new**.

- 2.1 Referring to the wording of **claim 1** document D1 discloses:

a method of obtaining secure registration by a memory module (SIM module of mobile M in figure 5; SIM being implicitly disclosed, as document D1 relates to wireless communication systems e.g. GSM or IS41; column 1, lines 7-9 and 53-55) in a multicast-broadcast-multimedia system (GSM or IS41 can be used also for multicast-broadcast-multimedia system), the method comprising:

- receiving a random number (R_T at M, figure 5);
- generating a radio access network key (K_A at M, figure 5) as a function of the random number (R_T at M, figure 5) and a key of a public land mobile network (K_i shared between M and HLR in figure 5; column 5, lines 40-43; column 5, line 56 - column 6, line 2).
- generating a temporary registration key as a function of the radio access network key (authentication response, figure 5; column 6, lines 5-8).
- generating a radio access network key (R_A at M, figure 5) as a function of the random number and a key selected from the group consisting of a public land mobile network key and a broadcast access key; and

Therefore the subject-matter of **claim 1** is not new.

- 2.2 The subject-matter of independent **claims 22 and 41** is representation of method claim 1 in terms of features of a memory module and a computer readable

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING
AUTHORITY (SEPARATE SHEET)**

International application No.

PCT/US2004/021530

medium capable to performing the method steps. Therefore, the argumentation of the point 2.1 applies mutatis mutandis also for these claims.

- 2.3 Independent claim 12 is written in such a broad way, that it is not novel over the standard authentication procedure in GSM systems (see e.g. document D2, paragraph 3):
a method of obtaining secure registration by a mobile station in a multicast-broadcast-multimedia system, the method comprising:
- receiving a random number from a radio access network (RAND received at mobile station, D2, paragraph 3);
 - transmitting the random number to a memory module (RAND transmitted to SIM, D2, paragraph 3); and
 - receiving from the memory module a temporary registration key based on the random number(receding SRES from SIM, D2, paragraph 3).
- 2.4 Furthermore it has to be stated that argumentation of point 2.1 applies also mutatis mutandis for the subject-matter of independent claim 12, as communication between SIM card and mobile terminal is implicitly disclosed in D1 (D1 relates to wireless communication systems e.g. GSM or IS41; column 1, lines 7-9 and 53-55).
- 2.5 The subject-matter of independent **claims 31 and 52** is representation of method claim 12 in terms of features of a mobile station and a computer readable medium capable to performing the method steps. Therefore, the argumentation of the points 2.3-2.4 applies mutatis mutandis also for these claims.
3. **Dependent claims 2-11, 13-21, 23-30, 32-40, 42-51 and 53-61** do not contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the Article 33(1) PCT in respect of novelty (Article 33(2) PCT) and/or inventive step (Article 33(3) PCT) for the reason that the subject-matter of said claims is either in principle directly derivable from the disclosure of the document D1 or represents simple design details which are generally known to the person skilled in the field of obtaining secure registration by a mobile station:
- 3.1 The additional features of using the identity module of mobile telephone is not new (D1, column 1, lines 7-9 and 53-55; D2, paragraph 3)

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING
AUTHORITY (SEPARATE SHEET)**

International application No.

PCT/US2004/021530

Thus the subject-matter of **claims 2, 8-9, 13, 18-19, 23, 32, 37-38, 42, 48-49, 53 and 58-59** is not new.

- 3.2 The additional feature of **claims 3-5, 14-15, 24-26, 33-34 and 43-45** of receiving a provisioning message from the authority providing the common key cannot be regarded as involving inventive step as it represents the well known measure in all authentication procedures.
- 3.3 The additional subject matter of other dependent claims contains only implementation details within the scope of the customary practice followed by persons skilled in the art, which are not inventive.